Guia de uso de Sistemas de Conferências e Reuniões Online

Fernando Frota Redigolo – LARC/PCS/EPUSP
fernando@larc.usp.br

1 Introdução 2
2 Zoom 2
2.1 Tipos de Usuários 3
2.2 Criação de Reuniões 3
2.3 Início da Reunião 4
2.4 Controle de Entrada de Participantes 4
2.5 Controles da Reunião 5
2.6 Controles de um usuário Individual 6
2.7 Encerramento de Reunião 7
3 ConferênciaWeb 8
3.1 Tipos de Usuários 8
3.2 Criação de uma comunidade 8
3.3 Início da Reunião 10
3.4 Controle de Entrada de Participantes 10
3.5 Controles da Reunião 11
3.6 Controles de um usuário Individual 12
3.7 Encerramento de Reunião 12
4 Google Meet 13
4.1 Tipos de Usuários 13
4.2 Criação de Reuniões 13
4.3 Início da Reunião Agendada 14
4.4 Controle de Entrada de Participantes 15
4.5 Controles da Reunião 15
4.6 Controles de um usuário Individual 15
4.7 Encerramento de Reunião 16
5 Recomendações Gerais 16
5.1 Considerações sobre conteúdos em sessões de web conferência 16
5.2 Cuidados com o Ambiente Doméstico 17

1 Introdução

Com a situação de quarentena e isolamento social, serviços de videoconferência/ webconferência (e.g., Google Meet, ConferênciaWeb da RNP, Cisco Webex, Zoom) começaram a ser usado de forma intensiva para reuniões virtuais com múltiplos participantes, e várias questões de segurança tem surgido.

Dentre os principais problemas de segurança que tem acontecido por configurações impróprias destacam-se:

- Usuários desconhecidos/indevidos entrando em reuniões abertas;
- Compartilhamento intencional de conteúdo impróprio (a.k.a., *Zoom-Bombing*);
- Participantes interferindo na participação de outros (e.g., desligando o microfone de outro participante ou mesmo removendo-o da reunião);
- Vazamento de Dados;
- Bugs nos softwares de videoconferência.

De forma resumida é possível elencar alguns cuidados básicos a serem tomados com estas ferramentas:

- Manter o software de conferência e browser atualizados (com o uso intensivo, problemas têm sido identificados semanalmente);
- Cuidados na hora de agendar/convidar os participantes (as permissões de cada participante podem depender de como é criada a reunião e os participantes são convidados);
- Usar mecanismos de controle para entrada na reunião, tais como senhas e/ou "salas de espera" (onde o usuário só entra na sala mediante aprovação, mesmo tendo senha);
- Monitorar os participantes e controlar suas permissões durante a reunião;
- Cuidados com os conteúdos compartilhados.

Como cada ferramenta tem as suas particularidades, este documento detalha como utilizar alguns destes sistemas de uma forma mais segura. As ferramentas contempladas neste momento são:

- Zoom Meetings;
- Google Hangout Meet;
- Serviço ConferênciaWeb da RNP (Rede Nacional de Ensino e Pesquisa).

O documento encontra-se organizado da seguinte maneira: nos capítulos 2, 3 e 4 são apresentados guias de uso das respectivas ferramentas Zoom, ConferênciaWeb e Meet, com um foco em segurança e controle, enquanto que o capítulo 5 apresenta considerações adicionais à segurança de ferramentas de videoconferência/ videocolaboração e do ambiente doméstico.

2 Zoom

O Zoom trabalha com o conceito de reuniões com identificadores estáticos ou dinâmicos, criados no instante do agendamento da reunião. Algumas as permissões são definidas no agendamento, outras durante a reunião, e dependem do tipo do usuário.

Tipicamente cada reunião tem um ID diferente sendo gerado, com exceção de 2 casos:

- Reuniões recorrentes, onde o mesmo ID é reutilizado para múltiplas reuniões (ex.: um ID para cada disciplina ou por curso);

- ID pessoal da reunião (fixo), associado ao usuário – uso não recomendado.

2.1 Tipos de Usuários

O Zoom define os seguintes tipos de usuário para uma reunião:

a) Anfitrião: quem cria a reunião, tem permissão completa sobre a mesma;

b) Anfitrião Alternativo: durante o agendamento de uma reunião o anfitrião pode dar permissão completa para um 2º usuário, que terá as mesmas permissões que ele naquela reunião, por meio da opção de anfitrião alternativo (os dois devem pertencer à mesma conta como, por ex.: a conta da Poli, e devem possuir um usuário do tipo Licenciado). Apenas o *Anfitrião* e o *Anfitrião Alternativo* podem abrir uma reunião agendada;

c) Participante da reunião: qualquer indivíduo participando da reunião. Suas permissões dependem do que for configurado pelo *Anfitrião*; o *default* é terem permissão de compartilhar seu próprio microfone e vídeo, bem como participar do chat;

d) Co-Anfitrião: durante a reunião o *Anfitrião* pode dar permissões para um participante ajudá-lo a gerenciar a reunião. Tem basicamente as mesmas permissões dos outros anfitriões, com exceção da permissão de abrir a reunião. Deve ser atribuído apenas a usuários confiáveis (ex.: professores, monitores, membros de banca, apresentadores);

2.2 Criação de Reuniões

Recomenda-se a criação de reuniões por agendamento na interface web do zoom, que oferece maiores opções de segurança. As seguintes opções são recomendadas para a criação de reuniões com controle dos participantes (tanto reuniões com ID único como reuniões recorrentes):

- ID da reunião: marcar *Gerar automaticamente*;
- Senha da reunião: marcar *Solicitar senha da reunião*;
- Vídeo do Anfitrião e dos Participantes: Desligados (apenas no início da sessão, depois eles poderão habilitar se desejado);
- Áudio: marcar *Áudio do Computador* (para evitar participantes não-identificados via linha telefônica);
- Habilitar entrada antes do anfitrião: desmarcar;
- Desativar o som dos participantes após a entrada: marcar;
- Habilitar sala de espera: marcar;
- Somente usuários autenticados podem ingressar: é interessante marcar caso se tenha certeza que todos os usuários têm conta no Zoom;

Uma vez criada a reunião a tela que se seguir indicará o endereço da reunião (Figura 1), que deverá ser copiado e disponibilizado de forma restrita, apenas com as pessoas necessárias à reunião, como por exemplo, dentro de uma área no Tidia-AE/Moodle/Classroom, um email ou mensagem de WhatsApp aos participantes da reunião (clicando-se em “Copiar o convite” será exibida uma tela com um texto para uso em e-mails).

Incluir URL: https://zoom.us/j/269942945?pwd=eCtwSHhhYllzSG5WNUd4NER5Zno5UT09 Copiar o convite

Figura 1: Endereço de uma Reunião Zoom

2.3 Início da Reunião

É sugerido que a pessoa responsável por abrir a reunião inicie-a alguns minutos antes do horário marcado, para a entrada e autorização dos usuários. Apenas o Anfitrião (quem agendou a reunião) ou o Anfitrião Alternativo podem iniciar a reunião.

Recomenda-se iniciar a reunião diretamente no software do Zoom, no botão de "Start" na lista de reuniões agendadas à direita (Figura 2);
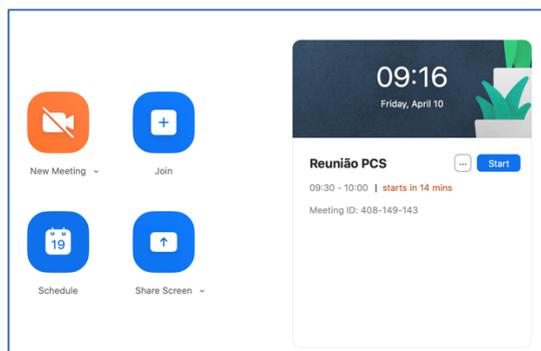
Figura 2: Início de Reunião Zoom

2.4 Controle de Entrada de Participantes

Uma vez iniciada a reunião, é necessário autorizar a entrada dos participantes. Com as configurações sugeridas anteriormente, o anfitrião receberá uma notificação a cada novo usuário na *Sala de Espera,* devendo ir na lista de participantes e clicar em "Admit" ou "Remove" conforme desejado (Figura 3) .
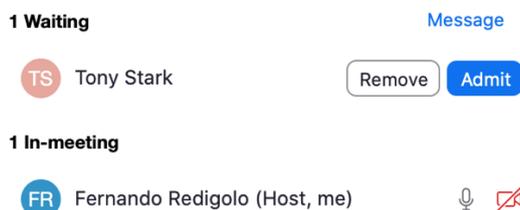
Figura 3: Admissão de usuários no Zoom

Caso sejam permitidos participantes sem login (não autenticado), a identificação do usuário é definida por ele, que pode colocar o que desejar (até o nome de outra pessoa), então deve-se ter cuidado ao aceitar os usuários (como, por exemplo, o usuário "Tony" na Figura 3). O Zoom permite uma validação por meio da opção "Message", para enviar um chat para quem estiver na sala de espera (Figura 4).
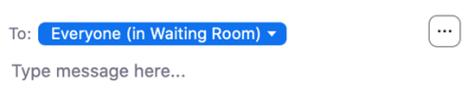
Figura 4: Chat para participantes na Sala de Espera do Zoom

Uma vez que todos os participantes estejam na reunião, o anfitrião pode opcionalmente travar a reunião, para não ser notificado de novos pedidos de entrada, indo no botão "Security" → "Lock Meeting" (Figura 5).
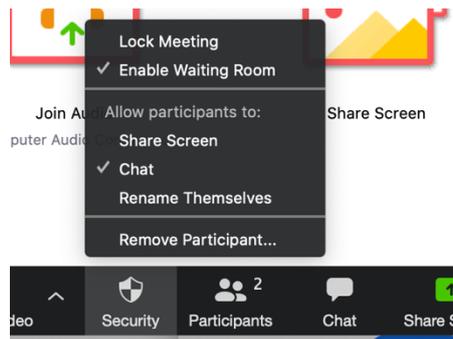
Figura 5: Travamento de Usuários no Zoom

2.5 Controles da Reunião

No botão Security (Figura 5) o Anfitrião pode desabilitar algumas funções para todos na reunião. Recomenda-se configurá-lo conforme visto na Figura 5:

- Share Screen: deixar desabilitado (e ativar conforme a necessidade ao longo da reunião);
- Chat: deixar habilitado (é possível restringir melhor em outro menu);
- Rename Themselves: deixar desabilitado.

Outras opções podem ser configuradas na lista de participantes, no botão "More" no final da lista de participantes (Figura 6)
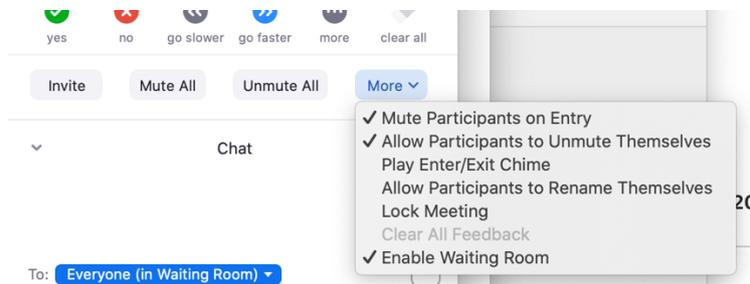
Figura 6: Opções de Controle para uma reunião em andamento no Zoom

Recomenda-se configurá-lo conforme as opções da Figura 6.

Em situações com um número muito grande de usuários como aulas e palestra é bastante comum o áudio dos participantes atrapalharem o andamento da apresentação. Neste caso é recomendável colocar todos em mudo (botão "Mute All" na lista de participantes - Figura 7). Em algumas situações é recomendável ainda fechar o áudio dos participantes, para interações apenas via chat, com a opção "Allow Participants to Unmute Themselves" tanto no botão "More" como em "Mute All"
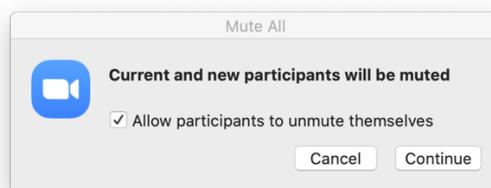
Figura 7: Mute All no Zoom

Em relação ao chat recomenda-se se possível a desativação de algumas funcionalidades para aulas e eventos com múltiplos participantes não-confiáveis, clicando-se no botão com "..." na janela de chat (Figura 8).
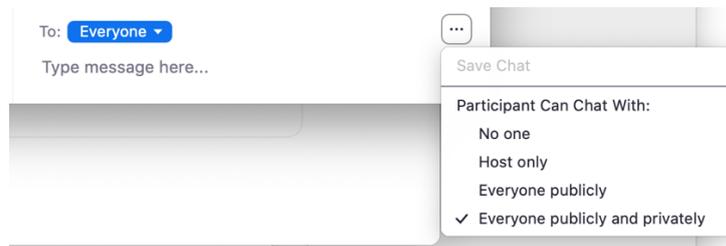
Figura 8: Controle de Chat no Zoom

Recomenda-se desativar a comunicação privada (entre dois participantes) em aulas e reuniões onde isso não seja necessário, deixando apenas a opção de mensagem para todos ("Everyone publicily"), ou mesmo permitir apenas mensagem ao ainfitrião ("Host Only").

2.6 Controles de um usuário Individual

Ao longo da reunião deve-se monitorar os participantes, de forma a desabilitar seu microfone, bem como para tirar da reunião pessoas que não deveriam participar da mesma ou que estejam com comportamento inadequado. Tais opções encontram-se ao lado do nome do participante ao ser apontado com o mouse (Figura 9).
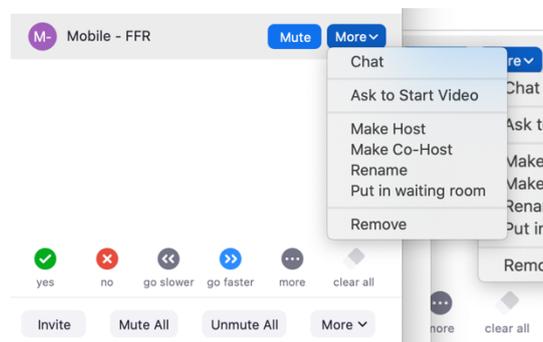
Figura 9: Controles de um usuário no Zoom

As seguintes opções são pertinentes:

- *Mute* – desligar o microfone do usuário;
- *Remove* – tirar o usuário da reunião definitivamente (ele não poderá mais entrar nesta sessão);
- *Put in waiting room* – tirar temporariamente o usuário da reunião (por ex.: para uma banca de mestrado discutir a aprovação de um candidato após a sua apresentação);
- *Make Co*-Host – transformar o usuário em um co-anfitrião

Para o compartilhamento de tela: ou se configura para que somente os Anfitriões tenham permissão (default) ou para todos os participantes. Desta maneira, para o compartilhamento recomenda-se:

- Transformar o usuário em co-anfitrião apenas quando necessário para o compartilhamento, e desativando depois (lembrando que, se ele não for confiável, terá controle completo neste período);

- Temporariamente ativar e desativar para todos (ex.: em uma aula onde os alunos estejam fazendo exercícios em seus computadores). Para tanto o Anfitrião deverá clicar na seta ao lado do botão de "Share Screen", selecionar "Advanced Sharing Options" e configurar as opções conforme a Figura 10. caso de compartilhamento por alunos ou pessoas não-confiáveis é possível apenas por meio da opção "All Participants" (recomenda-se portanto ativá-la apenas durante o período necessário);
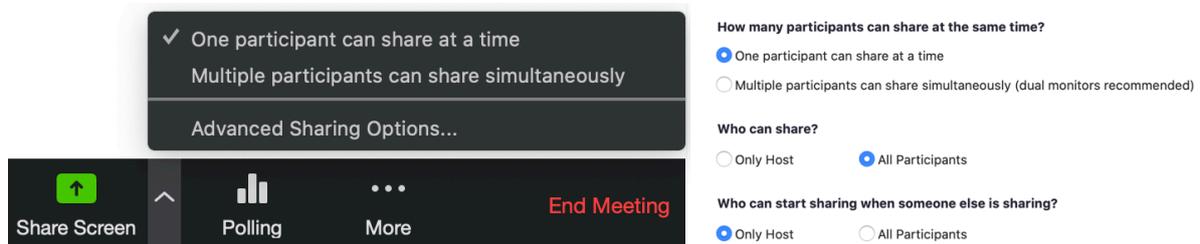
Figura 10: Controle de Compartilhamento no Zoom

2.7 Encerramento de Reunião

Caso algum usuário com permissões de controle necessite sair antes do término da reunião, deve-se prestar atenção para não derrubar a sessão no meio. Apenas o Anfitrião pode fechar a reunião. Quando ele clicar em "End Meeting" haverá a opção de decidir se fecha a sessão ou simplesmente sai, porém para sair é necessário transformar outra pessoa em Anfitrião, indo no menu de controle individual, opção "Make Host" (Figura 9).

3 ConferênciaWeb

O ConferênciaWeb trabalha com o conceito de comunidades estáticas, análogas a salas de reunião virtuais. Possuem identificadores fixos e conhecidos, ao contrário do Zoom e do Meet, que trabalham com IDs variáveis para cada reunião. O login é feito por meio da senha única do sistemas.usp.br, na opção Comunidade Acadêmica Federada – Café.

Há dois tipos de comunidades:

- Comunidade pessoal: criada automaticamente no primeiro login, só pode ser controlada pelo próprio usuário;
- Comunidades Públicas: deve ser criada manualmente, pode ser controlada por múltiplos usuários.

Um outro ponto é que o foco principal do ConferênciaWeb são apresentações de slides, complementadas por áudio/vídeo, diferentemente do Zoom e Meet, cujo foco principal são reuniões de áudio/vídeo. Desta maneira, apenas um usuário por vez pode fazer apresentações e compartilhar suas telas.

3.1 Tipos de Usuários

Os tipos de usuário em uma comunidade pública são:

a) Administradores: geralmente o criador da comunidade e outros autorizados por ele. Tem permissão completa sobre a mesma, incluindo mudar as permissões dos outros usuários;

b) Membros: pessoas com um *login* no serviço e que foram previamente cadastradas e aceitas para participar da comunidade. Tem permissão completa sobre a mesma, com exceção de aceitar novos membros e administradores. Recomenda-se que apenas pessoas confiáveis sejam incluídas como membros na comunidade (ex.: professores, membros de banca, membros de projeto);

c) Convidados: pessoas sem login no serviço ou usuários não-membros da comunidade. Permissão de compartilhamento de áudio/vídeo por default, outras permissões podem ser atribuídas pelos Membros ou Administradores durante uma reunião. Alunos ou pessoas não confiáveis devem ser colocadas nesta categoria;

d) Apresentador: pessoa que tem permissão de compartilhar a tela e controle sobre a reunião. Inicialmente é o usuário que abre a sala, porém esta permissão pode ser passada para os outros usuários da reunião (apenas um usuário por vez pode ser o apresentador).

3.2 Criação de uma comunidade

Recomenda-se sejam criadas comunidades públicas sempre que houver a necessidade de controle de múltiplos usuários ou que haja a possibilidade de conflito de utilização. De uma forma geral, as salas têm sido criadas para para disciplinas (ex.: PCS-3414), cursos (ex.: turmas de MBA), grupos de pesquisa/laboratório (ex.: LARC) e/ou departamentos (ex.: PCS).

Para a criação de uma comunidade basta definir um Nome, Descrição e Identificador (para o endereço web), conforme ilustrado na Figura 11, e marcar a sala como pública. O identificador será usado para o endereço web da comunidade; no exemplo o endereço da comunidade seria https://conferenciaweb.rnp.br/webconf/pcs-epusp.

Figura 11: Criação de comunidade no ConferênciaWeb

Após a criação deve-se configurar a forma de acesso, na aba Admin → Opções de Webconferência (Figura 12). Há duas opções possíveis:

- Acesso Privado: todos os usuários (membros e convidados) devem inserir uma senha para a participação na reunião, entrando diretamente na mesma (recomendada quando a comunidade é sempre usada pelos mesmos usuários – ex.: disciplinas e cursos);
- Acesso Público: usuários membros acessam a sala diretamente, enquanto que os convidados devem ser autorizados por um dos membros já presentes na reunião (recomendada quando a comunidade é usada por diferentes usuários ao longo do tempo – ex.: reuniões de projeto, reuniões de departamento);

Figura 12: Opções de Acesso a uma comunidade no ConferênciaWeb

O endereço que deve ser passado para todos os participantes da comunidade que pode ser visto na aba de webconferência da Comunidade (Figura 13).

Figura 13: Endereço para convite da Sala

3.3 Início da Reunião

É sugerido que a pessoa responsável por abrir a reunião (que deve ser um Administrador ou Membro da comunidade) inicie-a alguns minutos antes do horário marcado, para a entrada e autorização dos usuários. Ela deverá entrar na comunidade e clicar no botão "Iniciar" (Figura 14**Error! Reference source not found.**). No caso específico do Conferência Web a pessoa que abrir a sala inicia com a permissão adicional de apresentador.
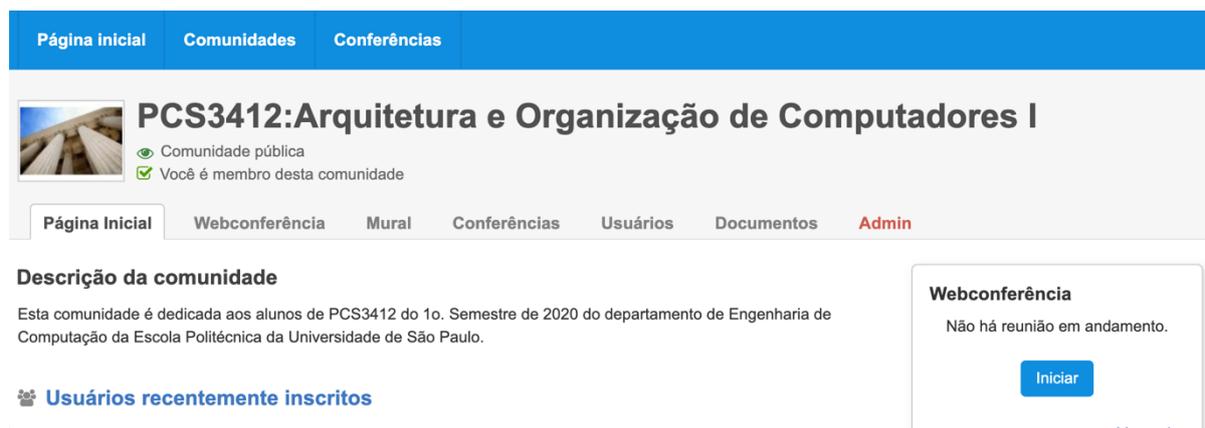
Figura 14: Início de Reunião no ConferênciaWeb

3.4 Controle de Entrada de Participantes

Caso a comunidade tenha sido configurada com a opção de acesso privado (como ilustrado na Figura 12) todos os usuários entram automaticamente após a digitação da senha correta, não sendo possível nenhum controle de entrada.

Caso ela tenha sido configurada como acesso público (com a opção "Privada" desmarcada na aba da Figura 12) todo acesso de não-membro gerará um pop-up e, na lista de participantes, haverá uma opção "Gestão de Utilizadores", onde será possível autorizar a entrada de cada usuário individualmente ou todos os pendentes de uma só vez. (Figura 15). Não marque a opção "Lembrar escolha", pois isso autoriza automaticamente usuários futuros a entrar na reunião.
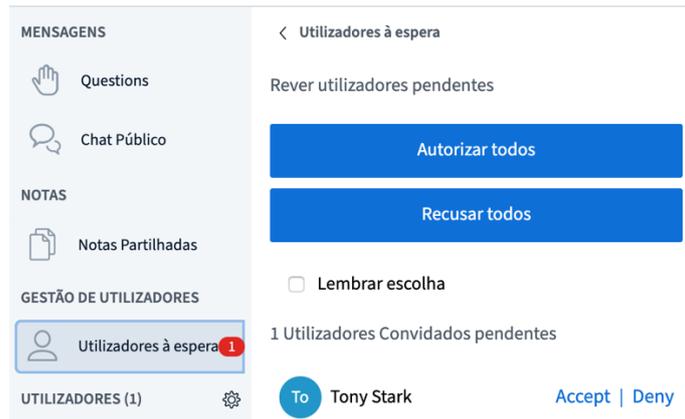
Figura 15: Autorização de entrada em comunidades com acesso público - ConferênciaWeb

Caso sejam permitidos participantes sem login (não autenticado), a identificação do usuário é definida por ele, que pode colocar o que desejar (até o nome de outra pessoa), então deve-se ter cuidado ao aceitar os usuários (como, por exemplo, o usuário "Tony Stark" acima).

3.5 Controles da Reunião

No ConferênciaWeb os controles da reunião podem ser encontrados ao se clicar na engrenagem ao lado de "Utilizadores" e selecionar a opção "Bloquear Participantes", conforme pode ser visto na Figura 16 (esquerda). Abrirá uma tela com as opções default de controle da reunião (Figura 16 – direita).
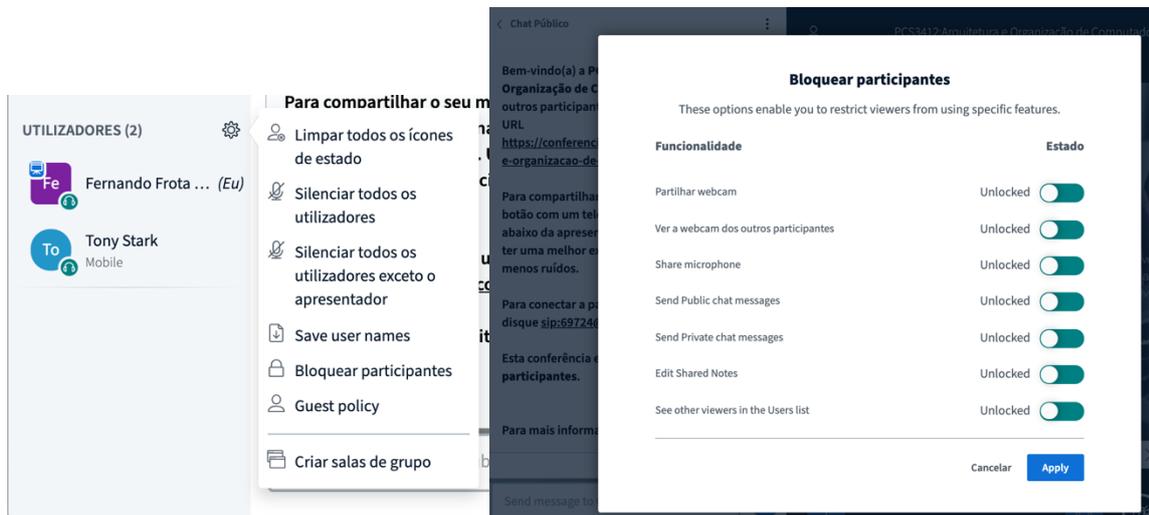
Figura 16: Controles Gerais da sessão

Recomenda-se:

- Desligar Microfones e webcams de participantes em palestras e aulas onde a interação se dará por chat apenas (menor possibilidade de áudio e vídeo interrompendo a reunião);
- Desligar a opção de Chat Privado para reuniões onde não é necessário que os participantes falem entre si sem a visão do apresentador.

Em situações com um número muito grande de usuários como aulas e palestra é bastante comum o áudio dos participantes atrapalharem o andamento da apresentação. Neste caso é recomendável colocar todos em

mudo, na opção “Silenciar todos os utilizadores exceto o apresentador” no menu ao lado de utilizadores - Figura 16 - esquerda).

3.6 Controles de um usuário Individual

Ao longo da reunião deve-se monitorar os participantes, de forma a desabilitar seu microfone, bem como para tirar da reunião pessoas que não deveriam participar da mesma ou que estejam com comportamento inadequado. Tais opções encontram-se no menu que aparece ao se clicar no nome do participante (Figura 17).
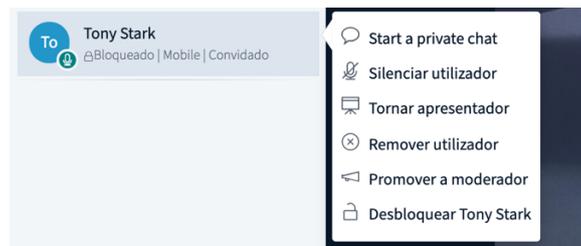
Figura 17: Opções de Controle Individual de participante - ConferênciaWeb

As seguintes opções são pertinentes:

- *Silenciar/Ativar microfone do utilizador* – desligar/ligar o microfone do usuário;
- *Tornar apresentador* – transformar o usuário em apresentador para que ele possa compartilhar tela ou controlar a apresentação de slides em PDF.
- *Remover utilizador* – remover o usuário da reunião (ele poderá entrar novamente na sessão);
- *Bloquear/Desbloquear <usuário>* – permitir que ele interaja na reunião com a câmera (só a pessoa pode ligar a câmera por questões de privacidade);

Somente uma pessoa por vez pode ser apresentador, então o apresentador atual deve utilizar a opção “Tornar Apresentador” para que outro possa controlar esta sessão.

3.7 Encerramento de Reunião

Caso algum usuário com permissões de controle necessite sair antes do término da reunião, deve-se prestar atenção para não derrubar a sessão no meio (qualquer membro tem permissão de encerrar a reunião na opção “Terminar sessão”).

4 Google Meet

O Meet trabalha com o conceito de reuniões instantâneas ou agendadas, com identificadores dinâmicos definidos no momento de criação ou agendamento da reunião. Possui um modelo mais simplificado de segurança, onde as permissões dependem essencialmente de como o usuário é convidado para a reunião e se o usuário pertence ou não ao @usp.br.

4.1 Tipos de Usuários

O Meet define os seguintes tipos de usuários:

a) Organizador da Reunião: quem agenda a reunião no Google Agenda, tem permissão completa sobre a mesma;

b) Criador da Reunião: quem inicia uma nova reunião instantânea diretamente pela interface do software, tem permissão completa sobre a mesma;

c) Convidados via Google: usuários com uma conta Google que são convidadas explicitamente de dentro do Google Agenda ou de dentro do Meet. Conseguem entrar diretamente na reunião;

d) Convidados via outros mecanismos: caso o usuário receba o link da reunião por outros canais diferente de um convite explícito (e.g.: por *copy-and-paste, forward* de em um email, WhatsApp, site, etc.). Estas pessoas necessitarão de aprovação caso não possuam login no Google ou seu login seja de fora do domínio @usp.br.

Se o usuário possuir conta @usp.br ele sempre entrará diretamente na conta, independente da forma que foi convidado;

4.2 Criação de Reuniões

No Meet uma reunião pode ser criada por meio do Google Agenda (reuniões agendadas) ou diretamente na ferramenta do Meet (reuniões instantâneas). Em ambos os casos poderá ser fornecido o endereço de email dos participantes, que poderão entrar diretamente na reunião. Estes usuários receberão um email enviado diretamente pelo Google para acesso à reunião.

Para a criação de uma reunião instantânea basta clicar no botão "Participar/iniciar reunião", colocar um nome para a reunião e clicar em "Participar Agora" (Figura 18). Será pedida a seguir o nome dos participantes que poderão entrar diretamente na mesma (Figura 19).
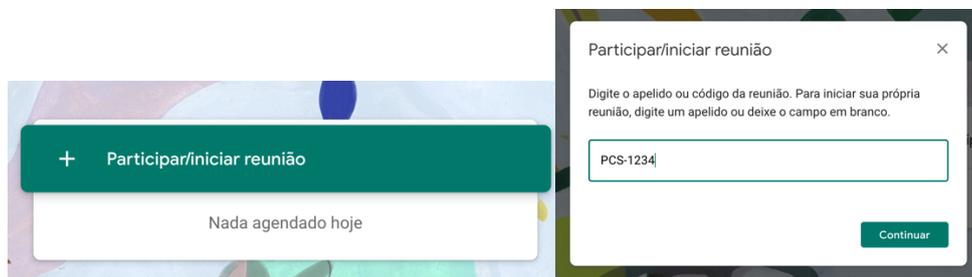
Figura 18: Criação de uma reunião instantânea no Meet
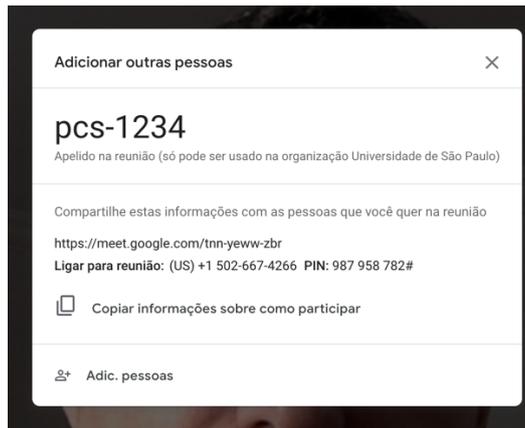
Figura 19: Adição de Participantes no Meet

Para o agendamento de uma reunião deve-se criar o evento no Google Agenda e clicar no texto "Adicionar Salas, Local ou Videoconferência" e, a seguir no texto "Adicionar conferência" para que seja criada uma reunião no Meet. Ao se clicar em "Adicionar Convidados" poderá ser feito o convite para aqueles que se deseja que entrem diretamente na sessão (Figura 20).
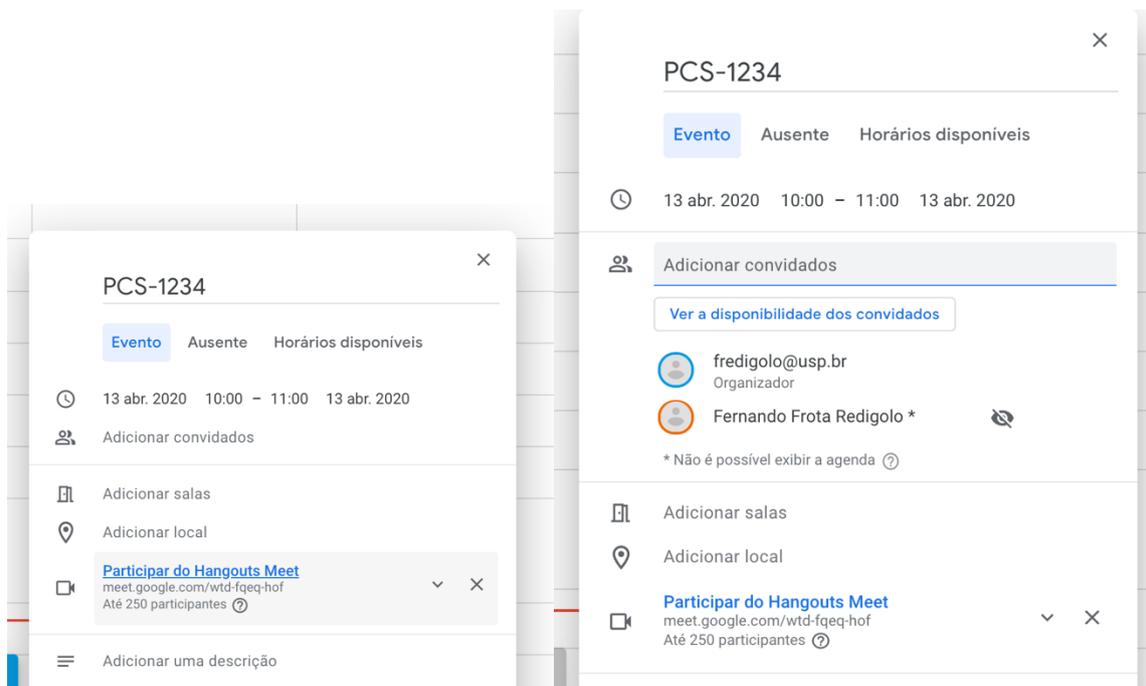
Figura 20: Tela de Aceite de usuários no Meet

4.3 Início da Reunião Agendada

É sugerido que a pessoa responsável pela reunião (criador ou proprietário do evento na agenda) inicie-a alguns minutos antes do horário marcado, para a entrada e autorização dos usuários de fora do domínio @usp.br.

No caso de reuniões agendadas, qualquer um dos usuários convidados diretamente poderá abri-la por meio do email de convite ou do link que aparece na tela inicial da ferramenta (Figura 21), porém apenas o proprietário terá permissões para autorizar usuários de fora do domínio @usp.br ou controlar os usuários da reunião.
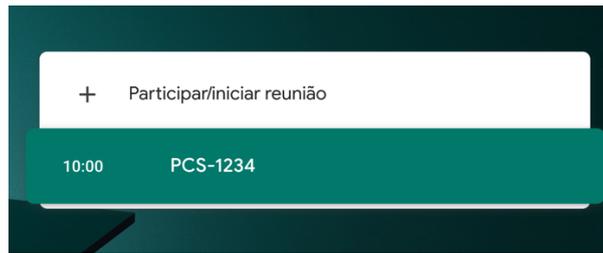
Figura 21: Início de reunião agendada no Meet

4.4 Controle de Entrada de Participantes

Uma vez iniciada a reunião, é necessário autorizar a entrada dos participantes que não foram convidados explicitamente (e que não possuam conta @usp.br), por meio do pop-up que irá aparecer apenas para o criador da reunião instantânea ou o organizador da reunião agendada (Figura 22).
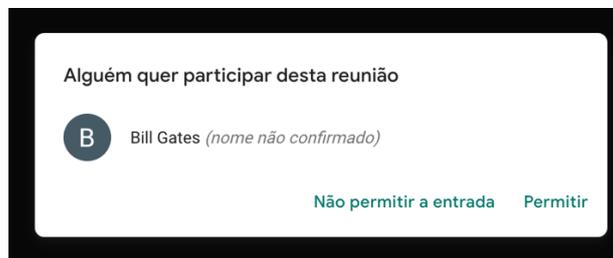
Figura 22: Aceite de usuários no Meet

É importante ressaltar que, no caso de participantes sem login na plataforma (não autenticado), a identificação do usuário é definida por ele, que pode colocar o que desejar (até o nome de outra pessoa). O Meet sinaliza esta situação com o texto "nome não confirmado", como pode ser visto na Figura 22.

4.5 Controles da Reunião

No Meet não há nenhum controle que possa ser feito a nível da reunião, como nos casos do Zoom e ConferênciaWeb (ex.: silenciar todos os participantes, bloquear novos participantes, entre outros). Todos os controles devem ser feitos por usuário.

Em particular, não é possível restringir o chat ou o compartilhamento de tela como nas outras plataformas citadas. O Meet apresenta o seguinte comportamento default:

- Compartilhamento de tela: se um usuário iniciar o compartilhamento, o compartilhamento anterior será interrompido e substituído;
- Chat: todas as comunicações do mesmo são enviadas para todos os participantes.

4.6 Controles de um usuário Individual

Ao longo da reunião deve-se monitorar os participantes, de forma a desabilitar seu microfone, bem como para tirar da reunião pessoas que não deveriam participar da mesma ou que estejam com comportamento inadequado. Tais opções aparecem ao se clicar no nome encontram-se no menu que aparece ao se clicar no nome do participante (Figura 23).
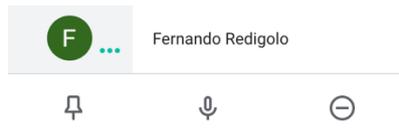
Figura 23: Opções de Controle Individual de participante - Meet

O Meet permite apenas silenciar o usuário (ícone do microfone na Figura 23) e remover o participante (ícone da direita na Figura 23). Somente o Criador ou o Organizador da reunião poderá efetuar estas operações.

4.7 Encerramento de Reunião

Não há uma opção explícita para encerrar uma reunião, ela termina quando todos os participantes saírem da mesma. Caso o Criador ou Organizador saia antes do término, ninguém poderá controlar outros participantes da reunião ou autorizar novas entradas.

5 Recomendações Gerais

5.1 Considerações sobre conteúdos em sessões de web conferência

Algumas recomendações adicionais sobre o conteúdo discutido em áudio/vídeo e sobre textos compartilhados nos chats:

- Em todas estas plataformas há criptografia para o conteúdo trafegado entre os usuários e os servidores, porém o conteúdo deve ser decriptado no servidor para a redistribuição aos outros usuários. Em tese, o provedor do serviço pode ter acesso ao conteúdo das reuniões;
- Considerar que vídeos e chats podem ser gravados pelos responsáveis pela reunião, de forma não-autorizada por um usuário com um software de captura de tela ou mesmo pelo provedor do serviço, e que estas informações podem vazar posteriormente, se não houver os devidos cuidados com a gravação. No caso do Zoom e do ConferênciaWeb há uma indicação visual de que a sessão está sendo explicitamente gravada pelo responsável;
- Cuidado com links compartilhados no chat fora de contexto, uma vez que podem ter sido inseridas por *malwares* na máquina de um participante autorizado, especialmente no caso de chats privados. Se o usuário não mencionou que iria compartilhá-la, procure confirmar com o participante se ele de fato a compartilhou;
- As reuniões e aulas virtuais são normalmente complementadas com conteúdos e aplicações compartilhadas em serviços de nuvem, como Google Drive, Dropbox, Google Docs, entre outros. Recomenda-se que o compartilhamento seja feito sempre para pessoas específicas e não seja usado compartilhamentos em que "Qualquer pessoa com o Link" pode acessar (em particular, no Google Drive da USP, a opção Gerar Link Compartilhável gera por default um compartilhamento deste tipo, aberto para qualquer pessoa na USP).

  A Figura 24 ilustra o compartilhamento recomendado em uma conta da USP no Google Drive.
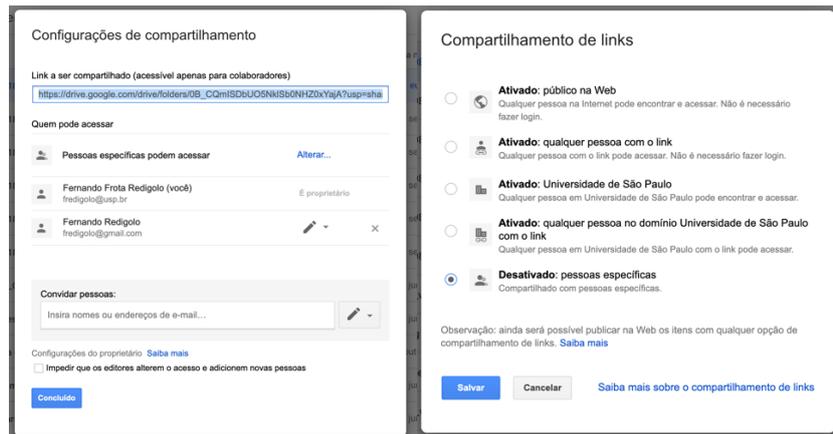
Figura 24: Controle de Compartilhamento de documentos no Google Drive

5.2 Cuidados com o Ambiente Doméstico

É interessante ainda reforçar alguns cuidados básicos com os ambientes domésticos que, em conjunto com as ferramentas de colaboração, tornaram-se os alvos preferenciais de ataques na conjuntura atual:

- Atualizar o sistema operacional e as aplicações na máquina usada para as reuniões virtuais. Em particular, vários bugs tem sido encontrados nestes ambientes de reunião virtual com o aumento de seu uso, e por isso seus respectivos clientes têm sido atualizados com uma certa frequência;
- Manter um backup da máquina, caso haja algum problema com a máquina sendo invadida, com sequestros virtuais (ramsomware) ou com algum update do sistema operacional (restaurar um sistema nestas condições por meio de suporte remoto é extremamente difícil);
- Usar soluções de segurança para desktop, como firewalls a antivirus/anti-malware;
- Verificar se o roteador doméstico está com uma senha default e se há atualização de seu firmware (os roteadores domésticos têm sido também alvo de ataques);
- Revisar as senhas usadas nos vários sites: evitando-se utilizar senhas de fácil descoberta e/ou reutilizar senha entre sites. Há diversas ferramentas que permitem o gerenciamento de múltiplas senhas, evitando-se o reuso de senhas, como o Lastpass, 1Password, Dashlane, entre outros. O site https://haveibeenpwned.com permite que se verifique se um determinado login já foi vazado e/ou se uma determinada senha já foi comprometida em vazamentos;
- Se possível utilizar autenticação em 2-fatores para serviços na nuvem, complementando a segurança da senha usual com um app para smartphone que gera códigos temporários e de uso único (OTP - One-Time Passwords), tais como o Google Authenticator, Microsoft Authenticator, entre outros;
- Nas condições atuais de Home Office o risco de distração é maior, e por isso, maior a chance de abrir uma mensagem ou link suspeito. Procurem ser criteriosos com links em mensagens recebidas em email, WhatsApp, entre outros (em particular, mensagens sobre Covid-19 tem sido usadas para invasões).